Item 2

23rd November 2022

Glasgow City Council

Strathclyde Pension Fund Committee

Report by Head of Audit and Inspection

Contact: Duncan Black Ext: 74053

INTERNAL AUDIT – Review of Information Management/Information Security

Purpose of Report:

To present the results of the Internal Audit review of the Information Management/Information Security arrangements within the Strathclyde Pension Fund Office.

Note:

In most cases one of four opinions is expressed:

1. The control environment is satisfactory i.e. audit testing found no concerns with the control environment.
2. A reasonable level of assurance can be placed upon the control environment i.e. audit testing found no major weaknesses in the control environment but some improvements could be made.
3. A limited level of assurance can be placed upon the control environment i.e. improvements are necessary to ensure the control environment is fit for purpose.
4. The control environment is unsatisfactory i.e. significant improvements are required before any reliance can be placed upon the control environment.

Recommendations:

The Committee is asked to note the contents of this report and **AGREE** the audit recommendation that the Head of Audit and Inspection submits a further report to Committee on the implementation of the actions contained in the Action Plan.

Ward No(s): Citywide: ✓

Local member(s) advised: Yes ☐ No ☐ consulted: Yes ☐ No ☐

Glasgow City Council Internal Audit Section
Committee Summary
Strathclyde Pension Fund Office – Information Management/Information Security Arrangements

1 Introduction

1.1 As part of the agreed Internal Audit plan, we have carried out a review of the arrangements for information management and information security within the Strathclyde Pension Fund Office (SPFO).

1.2 The SPFO holds a diverse range of information, including sensitive information in relation to pension payments, it is important that staff are aware of how to manage this information to ensure it is held appropriately and securely, particularly with the move to hybrid working arrangements.

1.3 The UK General Data Protection Regulation (GDPR) sits alongside the amended Data Protection Act 2018 and applies to data processing carried out by organisations operating within the UK. GDPR provides enhanced rights to service users on how their data will be used and requires that data must not be retained for longer than is necessary.

1.4 The purpose of the audit was to gain assurance that there are adequate arrangements in place for managing information across the SPFO. The scope of the audit included ensuring that:

- There is an approved Records Management Plan and that associated procedures for the management of information including (but not limited to) a records retention and disposal schedule are in place;
- Information security procedures are in place and available to staff;
- There are adequate processes in place in relation to records management and information security and these have been communicated to staff;
- The SPFO senior management team has an awareness of the nature and classification of information it holds and the owners responsible for the information;
- There are clear arrangements in place for records retention and disposal, including the arrangements for archiving information and secure disposal of sensitive or confidential information and these are being complied with;
- There are arrangements in place to ensure that GDPR requirements are being adhered to;
- Staff are aware of their roles and responsibilities in relation to records management and information security and appropriate training has been provided;
- Information Security related issues are reported to senior management and the Committee/Board;

- Information sharing/data processing arrangements with external third parties are in place;
- There are Information Security incident handling processes in place; and
- Adequate controls have been put in place as a result of hybrid working to ensure that information remains secure at all times.

2 Audit Opinion

2.1 Based on the audit work carried out a reasonable level of assurance can be placed upon the control environment. The audit has identified some scope for improvement in the existing arrangements and four recommendations which management should address.

3 Main Findings

3.1 We are pleased to report that the key controls are in place and generally operating effectively. A representative from Financial Services attends the Glasgow City Council (GCC) Information Security Board and other information management related working groups. Any information management/security requirements or changes resulting from these groups are communicated to the SPFO via the Financial Services Leadership Team (FSLT) members, which includes the Director of Pensions. Information security and management guidance is available to SPFO staff via the Connect intranet site. Regular information management updates, for example details of data security breaches are provided to senior management. GDPR requirements are discussed regularly via the Systems and Compliance Team meetings. The SPFO is included in the GCC's Records Management Plan.

3.2 However, our audit testing found that there are some areas of non-compliance. The Records Retention Schedule is dated 2018, is not an active document and no longer reflects current practice. It also does not cover the records disposal process within the SPFO. GDPR requires data to be held for no longer than is necessary, however there are no formal arrangements in place within the SPFO to ensure that the data it holds is reviewed regularly to identify information which should be disposed of.

3.3 Although the SPFO documented all personal data it holds, where it came from and who it is shared with as part of the Council's data mapping exercise undertaken in 2017/18, the data has not been reviewed since to ensure that it remains fit for purpose. All SPFO staff are required to complete mandatory information security/management training courses on GOLD, however we were unable to confirm that all staff had completed the courses due to complete and accurate reporting being unavailable. We were advised that no hardcopy information should be removed from the office, however evidence that staff have been advised of this requirement could not be provided.

3.4 Although the employers that require Data Sharing Agreements have been identified and agreements issued, some signed agreements have not been returned, including four larger employers such as local authorities. There is

currently an outstanding recommendation for this as part of the previous Information Management audit therefore no further recommendation will be made in relation to this.

3.5 A Data Breach process document is in place, however the document was last updated in 2018 and does not contain all necessary guidance. A data breach log is maintained by the SPFO, however we found that it is missing key fields, such as the date the breach occurred. Data breaches should be reported to two responsible officers within the SPFO, however there are no arrangements in place to ensure that these officers' mailboxes are checked for reported data breaches when they are out of office.

3.6 An action plan is provided at section four outlining our observations, risks and recommendations. We have made four recommendations for improvement. The priority of each recommendation is:

Priority	Definition	Total
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	0
Medium	Less critically important controls absent, not being operated as designed or could be improved.	4
Low	Lower level controls absent, not being operated as designed or could be improved.	0
Service Improvement	Opportunities for business improvement and/or efficiencies have been identified.	0

3.7 The audit has been undertaken in accordance with the Public Sector Internal Audit Standards.

3.8 We would like to thank officers involved in this audit for their cooperation and assistance.

3.9 It is recommended that the Head of Audit and Inspection submits a further report to Committee on the implementation of the actions contained in the attached Action Plan.

4 Action Plan

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: A Records Retention Schedule is in place.				
1	A Records Retention Schedule was drafted for the SPFO in 2018, however it was never finalised and issued to staff for implementation. Subsequently no formal arrangements are in place within the SPFO to ensure that the data it holds is reviewed regularly to identify information which should be disposed of. The Records Retention schedule also does not cover the records disposal process within the SPFO. These issues increase the risk that the relevant SPFO staff may be unclear on the arrangements for the management of records and are unaware of the correct processes to follow when disposing of sensitive or confidential information.	The Records Retention Schedule should be reviewed and updated to ensure that it reflects current practice and includes the disposal process. Thereafter, the document should be communicated to relevant staff. SPFO management should ensure that appropriate arrangements are put in place to ensure that record retention periods are complied with. This should include ensuring that responsibilities are formalised, and sufficient records are maintained.	**Medium**	**Response:** Accepted. SPFO will update the Records Retention Schedule to reflect current practices and issue to relevant staff upon approval. The contents of the document will be reviewed annually. **Officer Responsible for Implementation:** Principal Pensions Officer (Compliance) **Timescales for Implementation:** 31 March 2023

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Activity has been undertaken to document the type and source of personal data held by the SPF and with whom it is shared.				
2	The SPFO documented the personal information it holds, where it came from and whom it is shared with as part of the data mapping exercise undertaken by the Council in 2017/18, however the data has not been subject to regular review. This increases the risk that the information held may no longer reflect current practice.	SPFO management should ensure that the data mapping document is reviewed and updated to ensure that it is complete and fit for purpose.	**Medium**	**Response:** Accepted. SPFO management will review the data mapping document and update if appropriate. **Officer Responsible for Implementation:** Pension Scheme Manager **Timescales for Implementation:** 31 March 2023

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Staff have received appropriate guidance and training in relation to information management/information security.				
3	All SPFO staff are required to complete mandatory information security and information management training courses on GOLD, these include the Information Security, Data Protection and Introduction to Records Management training courses. Although we confirmed that staff have been requested to complete these courses, we could not verify that all staff had completed the courses as the reporting functionality in GOLD is not working properly and the reports produced are incomplete. We were advised that no hardcopy information should be removed from the office, however evidence that staff had been advised of this requirement could not be provided. This increases the risk that staff may be unaware of their responsibilities in relation to information security and information management.	Once complete and accurate reports are available for GOLD, SPFO management should confirm the completion rate of all mandatory information security/management courses. If completion rates are lower than expected, management should take steps to improve these. Management should issue an email to all staff reminding them that hardcopy information should not be removed from the office.	**Medium**	**Response:** Accepted. GOLD reports will be requested from CBS, when available the completion rate will be confirmed and if required appropriate action will be taken. Email has been issued to all staff to remind them that hardcopy information should not be removed from the office. **Officer Responsible for Implementation:** Principal Pensions Officer (Compliance) **Timescales for Implementation:** 31 December 2022

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: There are Information Security incident handling processes in place.				
4	Although a Data Breach process document is in place, it was last updated in 2018. The document also does not include the containment and recovery process that should be followed. Currently staff are not asked to report near misses to management, by doing so, it would help avoid a similar incident becoming a data breach as management could take action as necessary. A data breach log is maintained by the SPFO recording all data breaches reported, however we found that the content of the log could be improved as it does not contain the following fields: • A reference number. • The date the breach occurred. • Actions taken/lessons learned (we were advised that this is currently undertaken informally). Staff should report any data breaches to two responsible officers within the SPFO. Thereafter these officers send corresponding data breach forms to the GCC Data Breach team who determines whether the breach needs to be reported to the Information Commissioner's Office(ICO). However we found that there are no arrangements in place to ensure that these officers' mailboxes are	SPFO management should update the Data Breach process document to include the containment and recovery process and guidance in relation to reporting near misses to management. Thereafter the document should be communicated to all staff. The data breach log should be updated to include the fields noted within the observation. Management should ensure that appropriate arrangements are put in place to ensure that when the responsible officers are unavailable that all reported data breaches can be accessed and actioned.	**Medium**	**Response:** Accepted. SPFO will review the process document for reporting data breaches and bring it up to date in terms of current practice, including reference to near misses. We will also review the data breach log and update it to include the additional fields noted in the observation. **Officer Responsible for Implementation:** Principal Pensions Officer (Compliance) **Timescales for Implementation:** 31 December 2022

No.	Observation and Risk	Recommendation	Priority	Management Response
	checked for reported data breaches when they are out of office. If near misses are not reported, this increases the risk that action is not taken to avoid a similar incident becoming a data breach. Delays in reporting data breaches could make them more difficult to manage and could result in fines being imposed by the ICO.			

5 Policy and Resource Implications

Resource Implications:

Financial:	Internal Audit services are included within the Central Support Services cost.
Legal:	None
Personnel:	None
Procurement:	None

Equality and Socio-Economic Impacts:

Does the proposal support the Council's Equality Outcomes 2021-25? Please specify.	No specific proposals are included within this report.
What are the potential equality impacts as a result of this report?	No significant impact.
Please highlight if the policy/proposal will help address socio-economic disadvantage.	There are no equality impacts as a result of this report.

Climate Impacts:

Does the proposal support any Climate Plan actions? Please specify:	Not Applicable
What are the potential climate impacts as a result of this proposal?	Not Applicable
Will the proposal contribute to Glasgow's net zero carbon target?	Not Applicable
Privacy and Data Protection Impacts:	None

6 Recommendation

6.1 The Committee is asked to note the contents of this report and **AGREE** the audit recommendation that the Head of Audit and Inspection submits a further report to Committee on the implementation of the actions contained in the Action Plan.